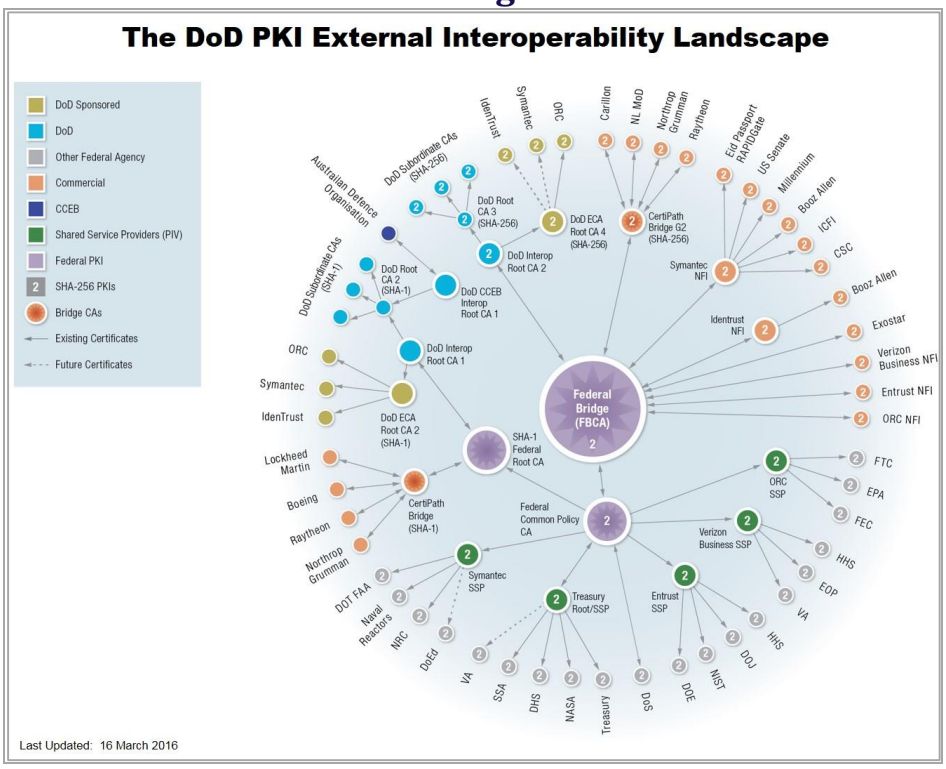
Working with External PKIs

Federal Information Sharing with partner PKIs

Over the past decade, the Department of Defense (DoD) has proven that Public Key Infrastructure (PKI) is a valuable asset for securing applications and networks. More recently, other federal agencies and industry partners have also implemented PKIs to protect their interests.

PKI interoperability is an essential component of secure information sharing between DoD and its partners within the federal government and industry. DoD application owners are permitted to accept certificates from DoD-approved external PKIs that have completed the requirements in the DoD External Interoperability Plan[1] (EIP). This is consistent with DoD instructions 8520.02[2] and 8520.03[3] and supports both DoD and federal initiatives to leverage common trusted credentials for secure information sharing such as HSPD-12[4], FIPS-201[5], and the Office of Management and Budget's (OMB) Requirements for Accepting Externally-Issued Identity Credentials memorandum[6].

Overview of the Federal Bridge



The Federal Bridge is a Certification Authority (CA) operated and maintained by the Federal PKI Management Authority that issues cross-certificates to other CAs. These cross certificates create trust relationships between the two CAs. These trust relationships can be combined to form a bridge of trust that connects people from different PKIs.

[1] http://iase.disa.mil/pki-pke/Documents/unclass-dod_xternal_interop_plan_082010.pdf
[2] http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf
[3] http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf
[4] http://www.idmanagement.gov/homeland-security-presidential-directive-12
[5] http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
[6] https://cio.gov/wp-content/uploads/downloads/2012/09/OMBReqforAcceptingExternally_IssuedIdCred10-6-2011.pdf

Partner PKIs Approved as of March 2016

Australian Defence Organisation PKI

Boeing PKI

Carillon Federal Services PKI

Department of State PKI

Entrust Managed Services NFI PKI

Entrust SSP PKI

Exostar PKI

IdenTrust NFI

Lockheed Martin PKI

Netherlands Ministry of Defence PKI

Northrop Grumman PKI

ORC NFI PKI

ORC SSP PKI

Raytheon PKI

Symantec NFI PKI
(formerly VeriSign NFI PKI)

Symantec SSP PKI
(formerly VeriSign SSP PKI)

US Treasury PKI

Verizon Business NFI PKI

Verizon Business SSP PKI

The full list of partner PKIs is available on the IASE at http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx

What are DoD Approved External PKIs?

DoD Approved External PKIs are PKIs that are approved for use within DoD but are managed outside of DoD PKI. The DoD External Interoperability Plan (EIP) defines three categories of external PKIs which may be approved for use within DoD and the requirements for becoming a DoD approved external PKI. The three categories are: Category I – US Federal Agency PKIs; Category II - Non-Federal Agency PKIs that are cross certified with the FBCA; Category III – Foreign, Allied, or Coalition Partner PKIs or other PKIs.

Which PKIs can I trust?

The authoritative list of DoD Approved External PKIs can be found on the DoD PKE site at http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx.

Why should DoD accept or trust other PKIs?

Use of External PKI credentials eliminates the need for DoD to issue DoD credentials to its partners. By leveraging federally issued and federally trusted identity credentials, DoD is supporting federal identity management initiatives to reduce costs and complexity associated with managing multiple identity credentials.

How do we implement trust for Partner PKIs?

Application owners or network administrators have two implementation choices for enabling trust for external PKI credentials: 1) Direct Trust Model or 2) Cross Certificate Model. More information can be found in the DoD PKI Interoperability White Paper located on the DoD PKE site at http://iase.disa.mil/pki-pke/Pages/index.aspx under *PKE A-Z*. Specific configuration information for common server products can also be found on the *PKE A-Z* page.

More Information

For more information about approval of additional external PKIs, please contact the External Interoperability Working Group EIWG at ExternalPKI.Interoperability@osd.mil.

For technical implementations or enablement of your DoD PK enabled application to accept external PKIs, contact DoD PKE Support at dodpke@mail.mil.

If you require a DoD PK-enabled application or network to use an approved external PKI, please contact the website, application or network administrator.

IMPORTANT NOTE: DoD information owners and application administrators should strongly consider whether they need to trust external PKI credentials. Extending trust to external PKIs should match business need to add external audiences to DoD systems. Administrators are advised to consult with their organization's DAA prior to configuring trust for any External PKIs.